UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,581	12/20/2001	Joseph M. Fontana	2356P	3274

7590 12/24/2003

SAWYER LAW GROUP LLP
P.O. Box 51418
Palo Alto, CA 94303

EXAMINER	
ELISCA, PIERRE E	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 12/24/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)
10/028,581	Joseph M. Fontana et al.
Examiner	**Art Unit**
Pierre E. Elisca	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *THREE* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *10/06/2003*.

2a) ☐ This action is **FINAL.** 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above, claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-3, 6-17, 20-22, 24-26, and 29-39* is/are rejected.

7) ☒ Claim(s) *4, 5, 18, 19, 23, 27, and 28* is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are a) ☐ accepted or b) ☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____
4) ☐ Interview Summary (PTO-413) Paper No(s). _____
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

RESPONSE To AMENDMENT

1. This Office action is in response to Applicant's RCE/Amendment, filed 10/06/2003.

2. Claims 1-39 are presented for examination.

CLAIM OBJECTION

3. Claims 4, 5, 18, 19, 23, 27, and 28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102 (b)

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 (b) that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-3, 6-17, 20-22, 24-26 and 29-39 are rejected under 35 U.S.C. 102 (b) as being anticipated by Chou et al. (U.S. Pat. No. 5,222,133).

As per claims 1, 3, 12, 16, 17, 20, 21 and 22 Chou discloses a method of protecting computer software from unauthorized users, comprising:

encrypting the software to be protected using an encryption key, creating encrypted software (see., abstract, specifically wherein it is stated that an algorithm for processing a plurality of keys including the first key in software, col 2, lines 31-54);

authorizing use of the software on the computer system by generating the encryption key within the security device using information supplied from the software (see., abstract, col 1, lines 26-53, specifically wherein it is stated that a first key (or encryption key) is stored in the program and a second key (or encryption key), physically separate from the program, is supplied to the customer with each program sold in a hardware based register. The first and second keys are compared to see if they bear a predetermined relationship to each other, in which case the program is authorized); and sending the encryption key from the security device to the computer system for decryption of the software (see., abstract, specifically wherein it is stated that the first and second keys in the algorithm for deriving a control key, please note that the control key is for decrypting the software since it is a part of the second key, and also col 1, lines 7-25, it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are parts of the control key, fig 1, specifically external computer or security device sending encryption key or software protected with algorithm to computer 14). Chou discloses using at least first and second pieces of information to generate an encryption key (see., abstract, please note that first and second pieces of information are readable as first and second keys, it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are parts of the control key). Chou discloses the claimed method of using an initialization vector (or first key)

and a dynamic key or second key as the first and second pieces of information (see., abstract, col 3, lines 23-39, col 4, lines 19-39, ID or encryption key or code). Chou discloses the claimed method of using a security key as the encryption key (or control key) and a communications key as the second encryption key (see., abstract). Chou discloses the software package has been loaded on the computer (see., Fig 1, items 20, 22 and 26). Chou further discloses a random number on the computer system (see., col 1, lines 41-53, please note that random number is readable as a pseudorandom number generator, and the authentication program see., Fig 1, software algorithm).

As per claim 2 Chou discloses the claimed method of using at least first and second pieces of information to generate an encryption key (see., abstract, please note that first and second pieces of information is readable as first and second keys);

associating the first piece of information (or first key) with the encrypted software (see., abstract, specifically wherein it is stated that an algorithm for processing a plurality of keys including the first key in software, col 2, lines 31-54); and

storing the second piece of information (or second key) in the security device (see., abstract, specifically wherein it is stated that a second key (or second piece of information), external to the software, to be protected which bears a relationship to the first key, col 2, lines 31-54).

As per claim 3, Chou discloses the claimed method of sending the first piece information associated with the encrypted software to the security device (see., abstract, specifically wherein it is stated that

an algorithm for processing a plurality of keys including the first key (or first information) in software, col 2, lines 31-54); and

using the first piece of information and the second piece of information to generate the encryption key in the security device (see., abstract, please note that first and second pieces of information is readable as first and second key, and the first and second keys in the algorithm for deriving a control key, please note that the control key (control key or encryption key) is for decrypting the software, and also col 1, lines 7-25, Fig 1).

As per claims 6, 13, 14, 15 and 20 Chou discloses the claimed method of using an initialization vector (or first key) and a dynamic key or second key as the first and second pieces of information (see., abstract, col 3, lines 23-39, col 4, lines 19-39, ID or encryption key or code).

As per claim 7, Chou discloses the claimed method of using a security key as the encryption key (or control key) and a communications key as the second encryption key (see., abstract).

As per claim 8, Chou discloses the claimed method of embedding a mathematical algorithm (fig 1, item 16, col 3, lines 23-39, mathematical algorithm or algorithm) within the security device to create the communication key (or proper key) and the security key (or newly control key) from the dynamic key (or second key) and the initialization vector or first key (see., abstract, col 3, lines 23-39).

As per claim 9, Chou discloses the claimed method of including the encrypted software with an authentication program, wherein the authentication program is embedded within a separate security processor provided in conjunction with the co-processor (see., abstract, col 3, lines 65-68, col 4, lines 1-39, Fig 1, item 16, please note that the algorithm of Fig 1 is an authentication program, and it is located within a separate security processor 16 or external computer).

As per claim 10, Chou discloses the claimed method of sharing memory between the security processor and the co-processor and decrypting the encrypted software in the shared memory (see., Fig 1, abstract, col 2, lines 31-54, col 3, lines 63-68, item 10, please note that the second key can be used to decrypt data in the shared memory since it is a part of the control key).

As per claim 11, Chou discloses the claimed method of preventing the software from running in any of the co-processor unless the software has first been decrypted by the security processor (see., abstract, col 4, lines 1-39, specifically wherein it is stated that if either or both of the two keys forming the unique key pair do not fit the algorithm as desired, a result which will occur which can be considered an error, also Fig 1, step 30 erroneous operation or wrong key which is used to stop the processing of the program).

As per claims 24, 27, 35 and 39 Chou discloses the claimed limitations of protecting computer software from unauthorized users, comprising:

encrypting the software to be protected using an encryption key, creating encrypted software (see., abstract, col 2, lines 31-54, please note that first and second pieces of information are readable as first and second keys, it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are part of the control key);

authorizing use of the software on the computer system by generating the encryption key within the security device using information supplied from the software (see., abstract, Fig 1, col 4, lines 20-39, specifically wherein it is stated that if output 32 is provided, this indicates that a correct code (or encryption key) exists, has been recognized, and thus will permit the continued processing of the protected software); and

sending the encryption key from the security device to the computer system for decryption of the software (see., Fig 1, specifically wherein it is stated that the first and second keys in the algorithm for deriving a control key, please note that the control key is for decrypting the software since it is a part of the second key, and also col 1, lines 7-25). Chou discloses wherein said initialization vector (or first key) is created from a checksum of encrypted software to be protected (see., fig 1, checksum or algorithm software, abstract, col 3, lines 23-39, col 4, lines 19-39, ID or encryption key or code). Chou further discloses decrypting the encrypted first encryption key on the computer using the second key included in the software (see., abstract please note that the control key is for decrypting the software since it is a part of the second key, and also col 1, lines 7-25, it is it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are parts of the control key).

As per claim 25, Chou discloses the claimed limitations using at least first and second pieces of information to generate an encryption key (see., abstract, please note that first and second pieces of information is readable as first and second keys);

associating the first piece of information (or first key) with the encrypted software (see., abstract, specifically wherein it is stated that an algorithm for processing a plurality of keys including the first key in software, col 2, lines 31-54); and

storing the second piece of information (or second key) in the security device (see., abstract, specifically wherein it is stated that a second key (or second piece of information), external to the software, to be protected which bears a relationship to the first key, col 2, lines 31-54).

As per claim 26, Chou discloses the claimed limitations of sending the first piece information associated with the encrypted software to the security device (see., abstract, specifically wherein it is stated that an algorithm for processing a plurality of keys including the first key (or first information) in software, col 2, lines 31-54); and

using the first piece of information and the second piece of information to generate the encryption key in the security device (see., abstract, please note that first and second pieces of information is readable as first and second key, and the first and second keys in the algorithm for deriving a control key, please note that the control key (control key or encryption key) is for decrypting the software, and also col 1, lines 7-25, Fig 1).

As per claims 29, 36, 37 and 38 Chou discloses the claimed limitations of using an initialization vector (or first key) and a dynamic key or second key as the first and second pieces of information (see., abstract, col 3, lines 23-39, col 4, lines 19-39, ID or encryption key or code).

As per claim 30, Chou discloses the claimed limitations of using a security key as the encryption key (or control key) and a communications key as the second encryption key (see., abstract).

As per claim 31, Chou discloses the claimed method of embedding a mathematical algorithm (fig 1, item 16, col 3, lines 23-39, mathematical algorithm or algorithm) within the security device to create the communication key (or proper key) and the security key (or newly control key) from the dynamic key (or second key) and the initialization vector or first key (see., abstract, col 3, lines 23-39).

As per claim 32, Chou discloses the claimed method of including the encrypted software with an authentication program, wherein the authentication program is embedded within a separate security processor provided in conjunction with the co-processor (see., abstract, col 3, lines 65-68, col 4, lines 1-39, Fig 1, item 16, please note that the algorithm of Fig 1 is an authentication program, and it is located within a separate security processor 16 or external computer).

As per claim 33, Chou discloses the claimed method of sharing memory between the security processor and the co-processor and decrypting the encrypted software in the shared memory (see.,

Fig 1, abstract, col 2, lines 31-54, col 3, lines 63-68, item 10, please note that the second key can be used to decrypt data in the shared memory since it is a part of the control key).

As per claim 34, Chou discloses the claimed method of preventing the software from running in any of the co-processor unless the software has first been decrypted by the security processor (see., abstract, col 4, lines 1-39, specifically wherein it is stated that if either or both of the two keys forming the unique key pair do not fit the algorithm as desired, a result which will occur which can be considered an error, also Fig 1, step 30 erroneous operation or wrong key which is used to stop the processing of the program).

RESPONSE TO ARGUMENTS

6. Applicant's arguments filed on 10/06/2003 have been fully considered but they are not persuasive.

REMARKS

7. In response to Applicant's arguments filed on 10/06/2003, Applicant argues that the prior art of record taken alone or in combination fails to disclose:

a. " Applicant argues that it is unclear what the Examiner considers analogous to the claimed encryption key". Based upon the foregoing rejection indicated above, it is believed that Chou

discloses a method for protecting computer software from unauthorized users, wherein the method also includes an algorithm for processing a plurality of keys, i.e encryption in software.

b. " authorizing use of the software on the computer system by generating the encryption key within the security device using information supplied from the software". As indicated above, Chou discloses in the abstract, col 1, lines 26-53 that a first key (or encryption key) that is stored in the program and a second key (or encryption key), physically separate from the program, is supplied to the customer with each program sold in a hardware based register. The first and second keys are compared to see if they bear a predetermined relationship to each other, in which case the software program is authorized).

c. " sending the encryption key from the security device to the computer system for decryption of the software". However, the Examiner respectfully disagrees because Chou discloses in the abstract that the first and second keys in the algorithm for deriving a control key, please note that the control key is for decrypting the software since it is a part of the second key, and also col 1, lines 7-25, it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are parts of the control key, fig 1, specifically external computer or security device sending encryption key or software protected with algorithm to computer 14).

c. "Control key is generated on the computer, rather than in the security device". As stated above, Chou discloses in the abstract that the first and second keys in the algorithm for deriving a control key, please note that the control key is for decrypting the software since it is a part of the second key, and also col 1, lines 7-25, it is inherent to recognize that the first key can be used to encrypt data and

the second key can also be used to decrypt data since they are parts of the control key, fig 1, specifically external computer or security device sending encryption key or software protected with algorithm to computer 14).

Conclusion

8. Any inquiry concerning this communication from the examiner should be directed to Pierre Eddy Elisca at (703) 305-3987. The examiner can normally be reached on Tuesday to Friday from 6:30AM. to 5:00PM.

If any attempt to reach the examiner by telephone is unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768.

Any response to this action should be mailed to:

Commissioner of patents and Trademarks

Washington, D.C. 20231

The Official Fax Number For TC-3600 is:

(703) 305-7687

Pierre Eddy Elisca

Patent Examiner

December 23, 2003